

Grupo de Trabajo en Red
Request for Comments: 2404
Categoría: Pila de Estándares

C. Madson
Cisco Systems Inc.
R. Glenn
NIST

Noviembre 1998

Traducción al castellano:

Agosto 2005

Hugo Adrian Francisconi

<adrianfrancisconi@yahoo.com.ar>

Uso de HMAC-SHA-1-96 en ESP y AH

Estado de este documento

Este documento especifica un protocolo de Internet en vías de estandarización para la comunidad de Internet y solicita debate y sugerencias para mejorarlo. Por favor, remítase a la edición actual de "Estándares de Protocolos Oficiales de Internet" (STD 1) para conocer el estado de estandarización y status de este protocolo. La distribución de este memorándum es ilimitada.

Aviso de Copyright

Copyright (c) Sociedad Internet (1998). Todos los derechos reservados.

Resumen

Este documento describe el uso del algoritmo HMAC [RFC-2104] en conjunto con el algoritmo SHA-1 [FIPS-180-1] como mecanismo de autenticación, para la Carga de Seguridad Encapsulada [ESP] y para la Cabecera de Autenticación [AH] dentro de IPsec. HMAC con SHA-1 proporcionan autenticación del origen de datos y protección de integridad.

Información adicional sobre otros componentes necesarios para implementaciones de ESP y AH es proporcionada por [Thayer97a].

1. Introducción

Este documento especifica el uso de SHA-1 [FIPS-180-1] combinado con HMAC [RFC-2104] como mecanismo de autenticación de claves dentro del contexto de ESP y AH. El propósito de HMAC-SHA-1-96 es asegurar que el paquete es auténtico y que no puede ser modificado en tránsito.

HMAC es un algoritmo de autenticación de clave secreta. La integridad de los datos y la autenticación del origen de los datos como es proporcionada por HMAC es dependiente del alcance de la distribución de la clave secreta. Si solamente el origen y el destino conocen la clave HMAC, esto proporciona autenticación del origen de los datos e integridad de los datos para los paquetes enviados entre las partes; si el HMAC es correcto, esto prueba que el HMAC a sido agregado por el origen.

En este documento, HMAC-SHA-1-96 es usado dentro del contexto de ESP y AH. Para más información de como varias partes de ESP (incluyendo mecanismos de confidencialidad) se unen para proporcionar servicios de seguridad, referirse a [ESP] y a [Thayer97a]. Para más información sobre AH, referirse a [AH] y a [Thayer97a].

Las palabras DEBE, NO DEBE, REQUERIDO, PODER, NO PODER, DEBERIA, NO DEBERIA, RECOMENDADO, PUEDE y OPCIONAL, cuando aparezcan en este documento, deben interpretarse como se describe en el [RFC-2119].

2. Algoritmo y Modo

El [FIPS-180-1] describe el algoritmo fundamental SHA-1, mientras que el [RFC-2104] describe el algoritmo HMAC. El algoritmo HMAC proporciona un marco para insertar varios algoritmos de hash como el SHA-1.

HMAC-SHA-1-96 opera sobre bloques de datos de 64 bits. Los requerimientos para el relleno están especificados en [FIPS-180-1] y son parte del algoritmo SHA-1. Si usted construye SHA-1 de acuerdo con [FIPS-180-1] no necesitará agregar rellenos adicionales para HMAC-SHA-1-96. Con respecto al "relleno del paquete implícito" como lo define [AH] no es requerido.

HMAC-SHA-1-96 produce un valor de autenticación de 160 bits. Este valor de 160 bits puede ser acortado como se describe en el RFC 2104. Para usarse con ESP o AH, un valor truncado usando los primeros 96 bits BEBE ser soportado. En el envío, el valor truncado es almacenado dentro del campo de autenticación. En la recepción el valor completo de 160 bits es calculado y los primeros 96 bits son comparados con el valor almacenado en el campo autenticación. Ninguna otra longitud del valor de autenticación es soportado por HMAC-SHA-1-96.

La longitud de 96 bits fue seleccionada porque es la longitud de autenticación por defecto como está especificado en [AH] y soluciona los requisitos de seguridad descriptos en [RFC-2104].

2.1 Funcionamiento

[Bellare96a] indica que "el funcionamiento (de HMAC) es esencialmente el de la función hash principal". Como este artículo no describe el funcionamiento, se a realizado el análisis de SHA-1, HMAC o HMAC combinado con SHA-1.

El [RFC-2104] describe una modificación de implementación que puede mejorar el funcionamiento por paquete sin afectar a la interoperatibilidad.

3. Material Clave

HMAC-SHA-1-96 es un algoritmo de clave secreta. A pesar de que ninguna longitud de clave fija es especificada en [RFC-2104], cuando se usa en ESP o AH una longitud de clave fija de 160 bits DEBE ser soportada. Longitudes de claves distintas de 160 bits no DEBEN ser soportadas (es decir solamente claves de 160 bits deben ser usadas por HMAC-SHA-1-96). Una longitud de clave de 160 bits fue elegida basándose en las recomendaciones del [RFC-2104] (es decir longitudes de claves menores a la longitud de autenticación debilitan la seguridad y claves más largas que la longitud de autenticación no incrementan la seguridad).

El [RFC-2104] discute los requerimientos sobre el material clave, incluyendo una discusión de requerimientos de aleatoriedad fuerte. Una función pseudo-aleatoria fuerte DEBE ser usada para generar la clave de 160 bits requerida.

Al momento en que se produjo este documento no hay claves débiles especificadas para el uso de HMAC. Esto no significa que no existan. Si, en algún momento, un conjunto de claves débiles para HMAC es identificado, el uso de estas claves débiles debe ser rechazado, seguido de una solicitud de reemplazo de claves o una negociación de nueva SA.

[ARCH] describe el mecanismo general para obtener el material clave cuando claves múltiples son requeridas para una única SA (por ejemplo cuando una SA ESP solicita una clave para confidencialidad y una clave para autenticación).

Para proporcionar la autenticación del origen de los datos, los mecanismos de distribución de claves deben asegurar que claves únicas sean asignadas y que estén distribuidas solamente a las partes participantes en la comunicación.

El [RFC-2104] hace la siguiente recomendación con relación al recambio de claves. Los ataques actuales no indican una frecuencia

específica para el cambio de claves ya que estos ataques son prácticamente impracticables. Sin embargo, la renovación periódica de las claves es una práctica de seguridad fundamental que ayuda contra debilidades potenciales de la función y claves, reduce la información disponible a un criptoanálisis y limita el daño de una clave expuesta.

4. Interacción con los mecanismos de cifrado de ESP

Al momento de la creación de este documento no hay temen conocidos que excluyan el uso del algoritmo HMAC-SHA-1-96 con ningún algoritmo específico de cifrado.

5. Consideraciones de seguridad

La seguridad proporcionada por HMAC-SHA-1-96 se basa en la fuerza de HMAC, y en menor grado, en la fuerza de SHA-1. Al momento de la creación de este documento no hay ataques criptográficos prácticos contra HMAC-SHA-1-96.

El [RFC-2104] indica que para que las "funciones hash sean mínimamente coherentes" el birthday attack, el ataque más fuerte conocido contra HMAC, sea impracticable. Para un bloque de hash de 64 bits tal como HMAC-SHA-1-96 un ataque incluyendo el procesamiento exitoso de bloques de 2^{80} no sería práctico a menos que se hubiera descubierto que el hash principal tuvo colisiones después de procesar bloques de 2^{30} . Un hash con tales características de resistencia débil a colisiones sería generalmente considerado inservible.

También es importante considerar que mientras que SHA-1 nunca fue desarrollado para ser usado como un algoritmo de clave hash, HMAC tuvo ese criterio desde el principio.

El [RFC2104] también habla de la seguridad adicional potencial que es proporcionada por el acortamiento del hash resultante. Las especificaciones que incluyen HMAC están fuertemente impulsadas a realizar este acortamiento de hash.

Como el [RFC-2104] proporciona un marco para incorporar varios algoritmos de hash con HMAC, es posible reemplazar SHA-1 con otros algoritmos tales como MD5. El [RFC-2104] contiene una detallada discusión sobre las fortalezas y debilidades de algoritmos HMAC.

Así como es cierto que para cualquier algoritmo criptográfico, parte de su fuerza recae en la correcta aplicación del algoritmo, la seguridad del mecanismo de administración de clave y su implementación, la fuerza de la clave secreta asociada y sobre la

correcta implementación de todos los sistemas participantes. El [RFC-2202] contiene vectores de prueba y ejemplos de código para asistir en la verificación de la exactitud del código HMAC-SHA-1-96.

6. Agradecimientos

Este documento deriva en parte de trabajos previos realizados por Jim Hughes, aquella gente que trabajó con Jim Hughes en la transformaciones combinadas DES/CBC+HMAC-MD5 ESP, la ANX participantes bakeoff, y los miembros del grupo de trabajo de IPsec.

También nos gustaría agradecer a Hugo Krawczyk por sus comentarios y recomendaciones acerca de ciertos textos criptográficos específicos en este documento.

7. Referencias

- [FIPS-180-1] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.
<http://csrc.nist.gov/fips/fip180-1.txt> (ascii)
<http://csrc.nist.gov/fips/fip180-1.ps> (postscript)
- [RFC-2104] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
- [Bellare96a] Bellare, M., Canetti, R., and H. Krawczyk, "Keying Hash Functions for Message Authentication", Advances in Cryptography, Crypto96 Proceeding, June 1996.
- [ARCH] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
- [ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload", RFC 2406, November 1998.
- [AH] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
- [Thayer97a] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.
- [RFC-2202] Cheng, P., and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", RFC 2202, March 1997.
- [RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8. Direcciones de Autores

Cheryl Madson
Cisco Systems, Inc.

EMail: cmadson@cisco.com

Rob Glenn
NIST

EMail: rob.glenn@nist.gov

9. Declaración de Copyright Completa

Copyright (C) The Internet Society (1998). Todos los derechos reservados.

Este documento y sus traducciones puede ser copiado y facilitado a otros, y los trabajos derivados que lo comentan o lo explican o ayudan a su implementación pueden ser preparados, copiados, publicados y distribuidos, enteros o en parte, sin restricción de ningún tipo, siempre que se incluyan este párrafo y la nota de copyright expuesta arriba en todas esas copias y trabajos derivados. Sin embargo, este documento en sí no debe ser modificado de ninguna forma, tal como eliminando la nota de copyright o referencias a la necesario en el desarrollo de estándares Internet, en cuyo caso se seguirán los procedimientos para copyright definidos en el proceso de Estándares Internet, o con motivo de su traducción a otras lenguas aparte del Inglés.

Los limitados permisos concedidos arriba son perpetuos y no serán revocados por la Internet Society ni sus sucesores o destinatarios.

Este documento y la información contenida en él se proporcionan en su forma "TAL CUAL" y LA INTERNET SOCIETY Y LA INTERNET ENGINEERING TASK FORCE RECHAZAN CUALESQUIERA GARANTIAS, EXPRESAS O IMPLICITAS, INCLUYENDO, PERO NO LIMITADAS A, CUALQUIER GARANTIA DE QUE EL USO DE LA INFORMACION AQUI EXPUESTA NO INFRINGIRA NINGUN DERECHO O GARANTIAS IMPLICITAS DE COMERCIALIZACION O IDONEIDAD PARA UN PROPOSITO ESPECIFICO.

Notas del Traductor

Las Siguientes palabras no han sido traducidas y su significado es el siguiente:

- . birthday attack (ataque del día de cumpleaños): El nombre deriva de la probabilidad de que dos o más personas en un grupo de 23 personas, compartan la misma fecha de cumpleaños es menor que 0.5, (conocida como paradoja del cumpleaños). El birthday attack es un nombre usado para referirse a una clase de ataque por fuerza bruta. Para una función hash que tiene como salida una cadena de 160 bits, es necesario recorrer entonces 2^{80} mensajes para poder encontrar dos con el mismo hash, o sea encontrar una colisión.

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en ingles de las palabra/s que se encuentran (en español) a la izquierda, debido a que NO ESTOY SEGURO de que sea la correcta traducción del termino o simplemente para que no se pierda el VERDADERO sentido del texto.

La referencia [DOI] descripta en este RFC (RFC 2410) hace referencia al RFC 2408 (ISAKMP) pero me parece que los autores realmente quisieron hacer referencia al RFC 2407 (IP Security Domain of Interpretation).

Esta presente traducción fue realizada por Hugo Adrian Francisconi para mi tarjado de tesis de "Ingeniero en Electrónico" en la Facultad U.T.N. (Universidad Nacional Tecnología) Regional Mendoza - Argentina. Si le interesa IPsec y quieres saber más podés bajarte mi trabajo de tesis, "IPsec en Ambientes IPv4 e IPv6" de <http://codarec6.frm.utn.edu.ar>, para el cual traduje varios RFCs al español relacionados con IPsec. Cualquier sugerencia debate o comentario sobre este presente tema o traducción será bien recibida en adrianfrancisconi@yahoo.com.ar

Se a realizado el máximo esfuerzo para hacer de esta traducción sea tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". El traductor no será responsable ante cualquier persona o entidad con respecto a cualquier pérdida o daño que pudiera resultar emergente de la información contenida en está traducción.

Derechos de Copyright Sobre Esta Traducción

Esta traducción tiene los mismos derechos que le RFC correspondiente traducido, con el aditamento de que cualquier persona que extraiga TOTAL o PARCIALMENTE esta traducción deberá hacer mención de esta presente nota de copyright y de los datos del traductor.

Datos del Traductor

Nombre y Apellido del Traductor: Hugo Adrian Francisconi
Domicilio: Carril Godoy Cruz 2801, Villa Nueva-Guay Mallen-Mendoza-
Argentina
Código Postal: 5500
Tel: 054-0261-4455427
E-mail: adrianfrancisconi@yahoo.com.ar